UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,477	02/22/2002	Richard Brown	B-4518 619564-1	8511

7590 01/09/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/080,477	BROWN ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/17/2005 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on October 17, 2005 has been entered. Claims 1-18 are pending. Claims 1-5,8-16, and 18 are also amended by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Helbig, Sr. (US 5,841,868), and further in view of McNabb et al (US 6,289,462 B1).

a. *Referring to claim 1:*

i. Helbig teaches:

(1) an assessor computing device (i.e., trusted computing system) receiving via the network **[i.e., Helbig's invention relates to computer systems, and more particularly to stand-alone computers or to local networks of computers (column 1, lines 3-5 of Helbig)]** a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor computing device updating via the network the trust policy of a second computing device in accordance with the report **[i.e., a trusted computing system according to the invention includes a general-purpose computing apparatus with a keyboard port adapted to be coupled to a keyboard, and which is responsive to signals applied to the keyboard port to perform its function. The system also includes a keyboard with a plurality of keys and an output port, for generating keyboard signals representing keystrokes at the output port of the keyboard. A dumb card reader is coupled to the output port of the keyboard and to the keyboard port of the computing apparatus. The dumb card reader is adapted for coupling a removable access control card to the keyboard output port and to the keyboard port of the**

computing apparatus, and in one embodiment of the invention is also arranged for powering the access control card. The system according to the invention also includes a plurality of removable access cards adapted to be coupled to the dumb reader. Each of the access cards includes memory adapted for storing personal identification information such as a personal identification number of the authorized user to whom the card is issued. Within the card, a comparator is coupled to the memory, for, in a first mode of operation, comparing the keyboard signals with the personal identification information stored in the card memory, and for, when the comparator matches the keyboard signals with the personal identification information, switching to a second mode of operation, and for, in the second mode of operation, coupling the keyboard signals to the keyboard port of the computing apparatus. The system is secure, even against an unauthorized person who gains control of an access card, because no keyboard signals reach the computer itself until the personal information is verified by the card. Only an access card, together with knowledge about the information stored in the card's memory, can provide access (column 2, lines 28-60 and Figure 1)].

ii. Although Helbig teaches a trusted computing system as shown in Figure 1, Helbig is silent about receiving the report from the authorized card users. On the other hand, McNabb teaches:

(1) A set of records that collectively provide documentary evidence of processing. The audit trail enables tracing of events forward from the original transactions to related records and reports, and backward from records and reports to their component source transactions (column 7, lines 29-33 of McNabb). For example, a user initiating a print request from a database application would initially be permitted access to only that portion of the database that the user is permitted to view based on their role. Each row of a database table may have an extended attribute reflecting the authorization level or role that is required to view that record. This may be defined at the row insertion point where the default permission for the row corresponds to the level of the user that inserted the row. In this manner, the report would determine

the role of the user to determine the level of the records that may be retrieved **(column 18, lines 52-62 of McNabb).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have combined the teaching of McNabb into Helbig's system in which security against unauthorized access is provided **(column 1, lines 5-6 of Helbig).**

iv. The ordinary skilled person would have been motivated to:

(1) have combined the teaching of McNabb into Helbig's system wherein to such a system having security features for enabling control over access to data retained in such a system.

b. *Referring to claim 2:*

i. McNabb further teaches:

(1) wherein the assessor computing device (i.e., trusted computing system) updates via the network **[i.e., Helbig's invention relates to computer systems, and more particularly to stand-alone computers or to local networks of computers (column 1, lines 3-5 of Helbig)]** the trust policies of multiple computing devices in accordance with the report **[i.e., referring to Figure 4, the security attributes of the process and file are already established. In addition, managers seeking to upgrade security on their systems are thus often forced to rely on vendor claims of security performance. As new software emerges and inevitable upgrades to existing software pour in, IS professionals typically assume that the vendors have a vested interest in the security of their products. Given the potential implications of security system failure, it is critical that managers concentrate on security solutions that have undergone independent evaluation, testing, and certification (column 3, lines 64-67 through column 4, lines 1-5)].**

c. *Referring to claims 3-8, 12-14:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

d. *Referring to claims 9-11:*

i. These claims have limitations that is similar to those of claims 1-4, thus they are rejected with the same rationale applied against claims 1-4 above.

e. *Referring to claim 15:*

i. McNabb further teaches:

(1) a requestor, for requesting the report from the first computing device **[i.e., referring to Figure 1, element 6].**

f. *Referring to claim 16:*

i. Helbig teaches:

(1) a receiver for receiving via the network **[i.e., Helbig's invention relates to computer systems, and more particularly to stand-alone computers or to local networks of computers (column 1, lines 3-5 of Helbig)]** a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device, and the system further comprising first and second computing devices, wherein at least the first computing device comprises a reporter for sending via the network a trustworthiness report to the assessor computing device and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter **[i.e., referring to Figure 2, and further details are met on column 3, lines 53-67 through column 4, lines 1-32].**

ii. Although Helbig teaches a trusted computing system as shown in Figure 1, Helbig is silent about receiving the report from the authorized card users. On the other hand, McNabb teaches:

(1) A set of records that collectively provide documentary evidence of processing. The audit trail enables tracing of events forward from the original transactions to related records and reports, and backward from records and reports to their component source transactions (column 7, lines 29-33 of McNabb). For example, a user initiating a print request from a database application would initially be

permitted access to only that portion of the database that the user is permitted to view based on their role. Each row of a database table may have an extended attribute reflecting the authorization level or role that is required to view that record. This may be defined at the row insertion point where the default permission for the row corresponds to the level of the user that inserted the row. In this manner, the report would determine the role of the user to determine the level of the records that may be retrieved **(column 18, lines 52-62 of McNabb).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have combined the teaching of McNabb into Helbig's system in which security against unauthorized access is provided **(column 1, lines 5-6 of Helbig).**

iv. The ordinary skilled person would have been motivated to:

(1) have combined the teaching of McNabb into Helbig's system wherein to such a system having security features for enabling control over access to data retained in such a system.

g. *Referring to claim 17:*

i. This claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

h. *Referring to claim 18:*

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

Response to Argument

4. Applicant's arguments filed October 17, 2005 have been fully considered but they are not persuasive.

Applicant argues that:

There is no suggestion or motivation, either in references themselves or in combined references and that the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior arts.

Examiner disagrees with applicant and still maintains that:

The combination of teachings between Helbig and McNabb teach the claimed subject matter. As a matter of fact, Helbig clearly discloses **a trusted computing system** includes a computer, responsive to signals applied to its keyboard port. The system includes a keyboard for generating signals representing keystrokes. A card reader is coupled to the keyboard and to the computer keyboard port. The card reader couples one of a plurality of removable access control cards to the keyboard and to the computer keyboard port. Each of the access cards includes memory for storing personal identification information of the user to whom the card is issued. Within the card, a comparator is coupled to the memory, for, in a first operating mode, comparing the keyboard signals with the personal identification information stored in the card memory, and for, when the comparator matches the keyboard signals with the personal identification information, switching to a second operating mode, in which it couples the keyboard to the keyboard port of the computer. The system is secure, even against an unauthorized person controlling an access card, because no keyboard signals reach the computer itself until the personal information is verified by the card. Only an access card, together with knowledge about the information stored in its memory, can provide access. The information cannot be retrieved from the card itself. The invention provides positive separation of the user's private information from the computer, and does not allow this user to gain access to the computer software unless the private sign-on information is provided during the start-up process (see Helbig's abstract). In addition, McNabb teaches a system and method for providing a trusted server which controls access to the execution of processes by applying file level extended sensitivity label attributes. The attributes are utilized to restrict execution of processes that are requested by comparing the extended attributes in addition to using standard file permission authorization. The system additionally may be used to provide controlled execution of commercially available software (see McNabb's abstract). Although Helbig teaches a trusted computing system as shown in Figure 1, Helbig is silent about receiving the report from the authorized card users. On the other hand, McNabb teaches a set of records that collectively provide documentary evidence of processing.

The audit trail enables tracing of events forward from the original transactions to related records and reports, and backward from records and reports to their component source transactions (column 7, lines 29-33 of McNabb). For example, a user initiating a print request from a database application would initially be permitted access to only that portion of the database that the user is permitted to view based on their role. Each row of a database table may have an extended attribute reflecting the authorization level or role that is required to view that record. This may be defined at the row insertion point where the default permission for the row corresponds to the level of the user that inserted the row. In this manner, the report would determine the role of the user to determine the level of the records that may be retrieved **(column 18, lines 52-62 of McNabb).**

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teachings between Helbig and McNabb is sufficient.

Helbig and McNabb do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
December 30, 2005

KIM VU
SUPERVISORY PATENT
TECHNOLOGY CENTER